REMARKS

Claims 1-32 are pending in the present application. Claim 17 has been amended to correct a minor typographical error. Claims 17 and 30-32 have been amended to further clarify the invention. No new matter has been added. Applicant believes that the present application is in condition for allowance, and respectfully requests reconsideration of the rejection in light of the remarks set forth below.

I. REJECTION UNDER 35 U.S.C. §101

The Office Action rejected claims 17 and 30-32 under 35 U.S.C. §101 because the claimed invention is allegedly directed to non-statutory subject matter. Specifically, the Office Action alleges that claims 17 and 30-32 are directed to non-statutory subject matter because nothing is done with the primary or secondary signatures, i.e. there is no end result with the signatures.

The secondary signature is used to generate the primary signature as indicated in the claims. The primary signature is used by the mobile station to authenticate the subscriber. Claims 17 and 30-32 have been amended to include "wherein the primary signature is conveyed to the mobile station for authenticating the subscriber." This is a clarifying amendment and does not narrow the scope of these claims.

II. REJECTION UNDER 35 U.S.C. §102

The Office Action rejected claims 17 and 30-32 under 35 U.S.C. §102(b) as being allegedly anticipated by U.S. Patent No. 5,371,794 issued to Diffie. The rejection is respectfully traversed in its entirety.

To anticipate a claim under 35 U.S.C. § 102(b), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the … claim." (see MPEP §2131).

The Office Action states that Diffie teaches every element of claims 17 and 30-32. Applicant respectfully disagrees with the characterization of Diffie for the following reasons.

Diffie discusses a method for providing a secure wireless communication link between a mobile nomadic device and a base computing unit. Diffie teaches a key change protocol between a mobile nomadic device and a base computing unit to prevent service type attacks. (Col. 10, lines 22-64). A change key message exchange may be initiated between either the base unit or the mobile device. Each participant in the protocol of Diffie generates a public key/private key pair. "The private key is kept securely by the owner of the key pair. The public key is submitted over a secure channel to a trusted Certification Authority (CA). The CA examines the relevant information to ascertain that the public key is indeed being presented by someone whose identity is known and who can be "trusted". Having submitted the public key, *the person submitting is assumed to be in a position to obtain credentials on behalf of the machine whose public key is being certified.* The CA will then issue a certificate to the person (who is acting on behalf of the machine). The certificate will contain a binding between the public key and a logical identifier of the machine (such as a machine name), in the form of a document digitally signed using the CA's private key." As the person submitting *the public key is assumed to be in a position to obtain credentials on behalf of the machine whose public key is being certified*, Diffie merely ensures a secure communication, it *does not authenticate* the subscriber. The secure communication in Diffie could be with anyone. (See Col. 6, lines 1-17)

This is further evidenced in Col. 5, lines 35-40 of Diffie which states that *user authentication is ruled out* as end to end mechanism are not stipulated. As a result of no user authentication, what is left "is node-to-node (or machine-to-machine) authentication, since those are the entities primarily communicating over the wireless link. *Machine-to-machine authentication is conceptually appropriate for a security protocol at the link layer*." In other words, the authentication takes place as to the machine itself and *not the user of that machine.*

By contrast, the present claimed invention is aimed at an apparatus for *authenticating* a *subscriber (i.e., a user and not a machine as in Diffie)* in a wireless communication system. The apparatus selectively generates "a secondary signature that is received from the mobile station". Applicant submits that "authentication" as claimed is distinct from the key change protocol described by Diffie. With authentication the verifier or apparatus is able to determine whether the mobile user device is who he says he is. By contrast, in encryption a recipient of encrypted data either decrypts or fails to decrypt data but does not provide the sender of the data any information about whether such recipient is valid or authorized. Consequently, Diffie fails to disclose the claimed authentication method.

Upon further review of the portions cited in the Office Action, there seems to be nothing in Diffie to even suggest a method for *authenticating* a *subscriber* by "generating a primary signature based upon a key that is held private from the mobile station and *a secondary signature that is received from the mobile station*" as claimed. The Office Action relies on Col. 8, lines 26

– Col. 9, line 7 for illustrating the limitation of generating a secondary signature as in the claimed invention. However, this section of Diffie is directed to mobile devices and base units verifying signatures to *verify the authenticity of a base unit and a mobile device*, respectively. Specifically that the base unit is not an impostor and that the mobile is not an intruder.

With respect to the base unit, if the signatures match th*e base unit is considered to be authentic* (not the subscriber as in the present claimed invention*)*. If the signatures do not match, the original message is suspected of being tampered with and the mobile will abort the connection attempt. (See Col. 8, lines 38-42) Comparing two signatures is different than generating a secondary signature as claimed.

With respect to the mobile device, the base unit *verifies the signature of the message* (not the subscriber as in the present claimed invention). If the signature is verified, then the mobile device is an authentic host. (See Col. 8, line 59-65) Verifying a signature is different than generating a secondary signature as claimed.

Consequently, Diffie fails to disclose the generation of a secondary signature as in the claimed authentication method.

Since Diffie does not teach at least the above elements of claims 17 and 30-32, Applicant submits that Diffie does not teach all elements of claims 17 and 30-32 and therefore, claims 17 and 30-32 are allowable.

For at least the foregoing reasons, Applicant respectfully submits that Diffie does not teach every element of the claims and requests a withdrawal of the rejection under 35 U.S.C. §102.

Applicant has reviewed the references made of record and asserts that the pending claims are patentable over the references made of record.

III. ALLOWED CLAIMS

Applicant notes with appreciation the Examiner's allowance of claims 1-16 and 18-29 and request that they be promptly issued.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Date: June 19, 2008

By: /Won Tae C. Kim/
Won Tae C. Kim, Reg. # 40,457
(858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502